(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43476 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 29/06

(21) International Application Number: PCT/EP00/11747

(22) International Filing Date:
24 November 2000 (24.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9929050.4 8 December 1999 (08.12.1999) GB

(71) Applicant *(for all designated States except US)*: **NOKIA NETWORKS OY** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HAUMONT, Serge** [FR/FI]; Riistavuorenkuja 3 B AS. 10, FIN-00320 Helsinki (FI). **RAJANIEMI, Jaakko** [FI/FI]; Lapinrinne 2 A 11, FIN-00180 Helsinki (FI). **NIEMI, Valtteri** [FI/FI]; Topeliuksenkatu 32 G 11, FIN-00290 Helsinki (FI). **HURTTA, Tuija** [FI/FI]; Kiskottajankuja 4 D 49, FIN-02660 Espoo (FI). **SITCH, Paul** [GB/FI]; Harakantie 20 A 3, FIN-02600 Espoo (FI). **UUSIKARTANO, Joanna** [FI/FI]; Puistotie 3 B2, FIN-02760 Espoo (FI).

(74) Agents: **STYLE, Kelda, Camilla, Karen** et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

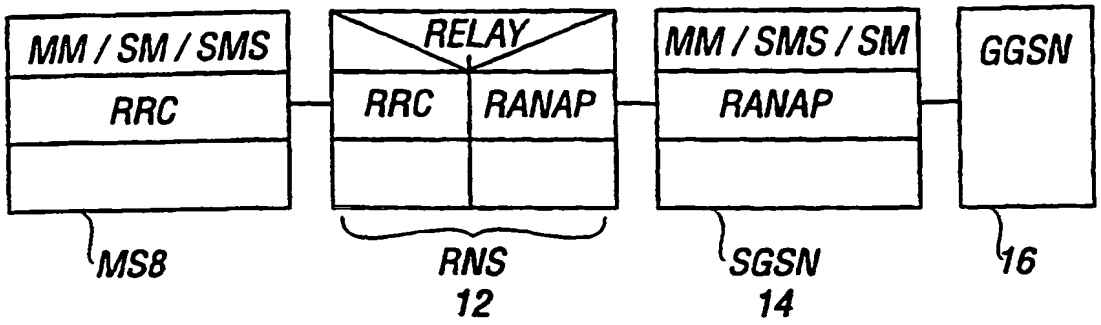
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COMMUNICATION METHOD



(57) Abstract: A method of communication between a first node, second node, and a third node comprising the steps of providing a message to be transmitted from one of the first and third nodes to the other of said first and third nodes, said message being sent through said second node: applying any required security procedure; determining if said message is to have a security procedure applied thereto in the first and/or the third node; and providing information relating to said security procedure.

WO 01/43476 A1

TITLE

COMMUNICATION METHOD

FIELD OF THE INVENTION

The present invention relates to a method of communication and in particular but not exclusively to a method of communication in a wireless cellular network for packet data. The present invention also relates to a communications system.

BACKGROUND TO THE INVENTION

The General Packet Radio Service GPRS standard relates to the transfer of data to and from mobile stations. The mobile stations are used in wireless cellular networks where the geographical area covered by the network is divided into a number of cells. Each cell has a base station, which communicates with mobile stations or other wireless terminals located in the cell associated with the base station. Typically, the GPRS standard is provided in conjunction with the Global System for Mobile communications GSM standard. The GSM standard relates to speech services. There are elements of the GSM standard and the GPRS standard which are in common. An adaption of the GPRS standard is also being proposed for use with the third generation standard UMTS, which uses code division multiple access.

In order to provide a secure call, which can not be intercepted by third parties, an authentication procedure is used to authenticate a user. Once a user had been successfully authenticated, the user is able to commence communicating with a

third party. For security purposes, these communications will be encrypted using a suitable encryption key. As a further security measure, an integrity check is also carried out using an integrity key. If an integrity check is performed and the check is not successful, the communication between the mobile station and the third party may be ended.

It has been proposed to apply ciphering and integrity checks in the UMTS system for the third generation standard. In this proposal it has been suggested that ciphering and integrity checks be applied to all communications between a mobile station and its associated base station. However, it has been recognised by the inventors that this gives rise to problems. In particular, if security measures are applied to some types of communications, the establishment of a connection may be prevented. A further problem is that the security measures may make the system unnecessarily sensitive and prevent connections from being established even where there is in practice no security problem.

SUMMARY OF THE INVENTION

It is an aim of embodiments of the present invention to address this problem.

According to a first aspect of the present invention, there is provided a method of communication between a first node, second node, and a third node comprising the steps of providing a message to be transmitted from one of the first and third nodes to the other of said first and third nodes, said message being sent through said second node; applying any required security procedure; determining if said message is to have a security procedure applied thereto in the first and/or the third node; and providing information relating to said security procedure.

The information relating to the security procedure may comprise information as to the applied security procedure or as to the required security procedure. The

information may be provided between the first and second nodes and/or the second and third nodes.

The security procedure may be an encryption procedure and/or an integrity check.

Embodiments of the present invention can be used in a communication network, such as a wired or wireless communications network. The preferred embodiments of the present invention are used in a cellular telecommunications network.

According to a second aspect of the present invention, there is provided a communications system comprising a first node and a second node and a third node, at least one of said first and third nodes via said second node, being arranged to transmit a message to be transmitted to the other of said first and third nodes; the transmitting node having means for determining if said message is to have a security procedure applied thereto, means for applying any required security procedure to said message, and means for providing information relating to said security procedure.

According to a third aspect of the present invention, there is provided a node for use in a communications system, said node being arranged to transmit a message from one node to another node, said node having means for receiving information relating to a security procedure to be applied to the message, means for applying said security procedure and means for transmitting the message to the another node.

According to a fourth aspect of the present invention, there is provided a node for use in a communications system, said node comprising means for transmitting a message from one node to another node, said node receiving information relating to a security procedure applied to said message, and means for advising the another node of said security procedure.

According to a fifth aspect of the present invention, there is provided a method of communication between a first node, a second node and a third node comprising the steps of providing a message to be transmitted from one of the first and third nodes to the other of the first and third nodes, said message being sent through said second node; providing said second node with information associated with said message, said second node being arranged to read said information but not said message; and providing a function associated with said information, if required.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention and as to how the same may be carried into effect, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 shows a cellular network with which embodiments of the present invention can be used;

Figure 2 shows in more detail the elements of the network shown in Figure 1;

Figure 3 shows schematically, the security procedure embodying the present invention; and

Figure 4 illustrates schematically the integrity check procedure.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Reference will be made to Figure 1, which shows a typical cellular network 2 with which embodiments of the present invention can be used. The area covered by the network is divided into a plurality of cells 4. Each cell 4 has associated therewith a base station 6. Depending on the standard being used by the network, the base station is sometimes referred to as node B, for example in the third generation standards. The term base station will be used in this document to

encompass all elements which transmit to mobile stations or the like via the air interface. In each cell 4, there are mobile stations 8 or other user equipment which is arranged to communicate with the respective base station associated with that cell.

The embodiment of the invention is described in the context of a UMTS (Universal Mobile Telecommunications System) which is concerned with communications involving packet data. In particular embodiments of the present invention are applicable to the proposals for the UMTS standard for the third generation systems. However, it should be appreciated that embodiments of the present invention are applicable to any other system which deals with packet data, non packet data or even voice communication or the like.

Reference will now be made to Figure 2 which shows the elements of a UMTS system in more detail. The mobile stations or user equipment 8 are arranged to communicate via the air interface with a respective base station 6. The base station is controlled by a radio network controller RNC. The radio network controller RNC and the base station are sometimes referred to as the radio network subsystem RNS 12.It should be appreciated that each radio network controller is arranged generally to control more than one base station 8 although only one base station is shown in Figure 2. The elements of the RNS can be included in either or both of the RNC and the base station. This is an implementation issue.

The radio network subsystem 12 is connected to a SGSN (serving GPRS support node) 14. The SGSN 14 keeps track of the mobile station's location and performs security functions and access control. The functions of the SGSN are defined in the 3GPP standard 33.060. The SGSN 14 is connected to a GGSN (gateway GPRS support node) 16. The GGSN 16 provides interworking with external packet switched networks. The GGSN thus acts as a gateway between the GPRS

network and an external network. Again the functions of the GGSN are defined in the 3GPP standard.

In the proposal for the GPRS standard for the third generation, the SGSN 14 and the mobile station have a upper layer L3 which supports mobility management MM and session management SM. This upper layer also supports the short message service SMS. The mobility management function manages the location of the mobile station of the mobile station, that is attachment of the mobile station to the network and authentication. Thus MM supports mobility management functionality such as attach, detach, security and routing updates. SMS supports the mobile-originated and mobile-terminated short message service described in the third generation standard UMTS 23.040.

The SGSN 14 and RN5 12 have a Radio Access Network Application Protocol (RANAP) layer. This protocol encapsulates and carries higher-layer signalling. RANAP handles the signalling between the SGSN 14 and the RNS12. RANAP is specified in the third generation standard UMTS 25.413. The mobile station 8 and the RNS 12 both have a radio resource control RRC which provides logical link control over the radio interface for the transmission of higher layer signalling messages and SMS messages. This layer handles the communication between the mobile station 8 and the base station.

MM, SM and SMS messages are sent from the SGSN 14 to the RNS 12 using the RANAP protocol. The packet is forwarded by the RANAP layer of the RNC 12 to the RRC layer of the RNC. The relay function in the RNS 12 effectively translates the message into a suitable form, that is into a RRC message for the mobile station 6. The MM messages are not read by the RNS. In embodiments of the invention, the RNS 12 checks associated information as to whether or not the RNS should cipher or integrity check the packet of the MM message. This will be

described in more detail hereinafter. The base station forwards the packet via the air interface to the mobile station 8.

In the mobile originated direction, the RRC layer of the mobile station 6 receives the MM message and sends it to the RNS12. The message is relayed from the RRC layer to the RANAP layer of the RNS. The RNS checks associated information with the message to see if the packet has been integrity checked and/or ciphered and in embodiments of this invention advises the SGSN 14 of the results of its check. It should be appreciated that the RNS is again not aware of the content of the MM message itself, only the associated information.

Reference will now be made to Figure 3 which shows the procedure when a mobile station attaches to the network.

In the first step S1, the mobile station makes an attach request. This for example may occur when the mobile station is first switched on or when the mobile station want to be attached to a network. This message is forwarded to the SGSN 14, the RNS 12 being transparent to this attach message.

In the second step S2, the SGSN 14 sends a message to the mobile station requesting information as to the mobile station's identity. This message is again sent transparently via the RNS 12. The SGSN 14 then checks to see if the mobile station 8 is permitted to attach to the network. The identity check may be omitted in alternative embodiments of the invention. The identity check may in alternative embodiments of the invention be carried after checking to see if the mobile station is permitted to attach.

In the third step S3, the mobile station 8 sends its IMSI (International mobile subscriber identity) to the SGSN 14 via the transparent RNS 12.

In the fourth step S4, the SGSN 14 forwards the IMSI to an authentication centre (not shown) which looks up an associated user's authentication key k. Using the authentication key k, the IMSI, and a random number RAND, a signal response SRES is generated. The SGSN 14 forwards the random number RAND to the mobile station along with a request for authentication of the user.

In step five S5, the mobile station uses the random number RAND and its IMSI and authentication key K which are both stored in the mobile station to generate a signal response SRES. The value of the signal response SRES calculated by the mobile station is sent to the SGSN 14.

In the sixth step S6, the SGSN compares the signal response SRES calculated by the mobile station with the signal response SRES calculated by the authentication centre and stored in the SGSN 14. If the values are the same, the mobile station is authenticated. The authentication centre is also arranged to calculate an encryption key Ck for the mobile station from the random number RAND and the user's authentication key. In addition an integrity key Ik is calculated. The integrity key is a function of (RAND,k). K is the long term shared secret between the authentication centre and the SIM card of the mobile station. The integrity checks which can be performed will be described in more detail later. The integrity key Ik and the cipher key Ck are forwarded to the radio network controller in a security mode command message (RANAP message). The security control command messages indicate whether or not to start ciphering. It is not ciphered but is integrity checked The RNC 10 stores the cipher key Ck and the integrity key.

The mobile station in step S7, also calculates the cipher key Ck from the information which is stored in the mobile station. The RNS 12 causes a security

control command message to be sent to the mobile station, which is integrity checked with the integrity key Ik.

In step S8, the mobile station generates an integrity checked response to a RRC message which is the security control responses using the integrity key Ik, which it has calculated and forwards it to the RNS 12

In step S9 the RNS 12 receives the signals from the mobile station and checks the integrity. If the integrity is in tact the RNS 12 informs the SGSN 14 that security protection was successful and all subsequent communication can be encrypted and integrity checked.

Before describing the integrity check in more detail, reference will be made to steps S10 to S13, which describe a communication between the SGSN 14 and the mobile station 8 which can be encrypted and/or integrity checked if required.

The SGSN 14 sends in step S10 a RANAP direct transfer message which is intended for the mobile station along with encryption indication field and an integrity indication field. The encryption indication field indicates if the L3 message MM, SM or SMS) is to be encrypted whilst the integrity indication field indicates if the L3 message is to be integrity checked.

In step S11, the RNS 12 receives the message along with the encryption indication and integrity indication fields in RANAP header. The RNS 12 does not look at the L3 message but does check the fields.RANAP direct transfer messages carry MM/SM/SMS messages and the proposed integrity and encryption indication fields are in RANAP level. Thus, the indication fields only need to be in the RANAP direct transfer message. In particular, the RANAP layer of the RNC receives the message and the fields. The fields are included in the RANAP header with the message being in the body of the packet. The message is passed from the RANAP layer of the RNS to the RRC layer of the RNS along

with the fields. If encryption is required, then the message is encrypted by the RNS and transmitted to the mobile station. If an integrity check is required, the RNS does the integrity check before sending the message to the mobile station. The MS when receiving the RRC message will decrypt it and check the integrity field.

In step S12, the mobile station receives the message and decrypts it if required. The mobile station also checks to see if the message was integrity checked. If so, the mobile station carries out its own integrity check and compares that result with the result received from the RNS to see if the integrity check is successful. In more detail the message and fields from the RNS 12 are received by the RRC layer of the mobile station. The RRC layer checks the fields to determine if the message is ciphered or integrity checked. The RRC layer then indicates to the L3 layer (e.g. MM) if the message is ciphered and/or integrity checked. The MM layer then checks to see if this is permitted for the message in question. For example, an authentication request will be accepted without any integrity check or ciphering. A routing area update response will be rejected if it was not integrity checked and ciphered.

The mobile station 8 is also arranged to send a message to the SGSN. The message is transmitted to the RNS 12. The MS sends message encrypted or not, and integrity checked or not. The receiving RRC entity can notice if the message is encrypted or not and integrity checked or not. If the message has been integrity checked, the value calculated by the integrity check is also transmitted to the RNS 12. In the RRC, the presence of this value is enough to provide the indication that the message has been integrity checked. In more detail, each time a MM message is provided to the RRC layer there is the indication as to whether the message shall be encrypted and/or integrity checked. The RRC entity in the MS transmits the message with encryption if required and integrity checks the message if required.

In step S13, the RNS 12if the message has been encrypted. If so, then the message is decrypted. If the message has been integrity checked, the RNS 12 carries out an integrity check and compares the result of that check with the result received from the mobile station. The message is then forwarded to the SGSN 14 along with an indication if the message has been integrity checked, and/or ciphered. In more detail, the RRC layer of the RNS 13 receives the transmission from the mobile station and checks the fields to see if the message was integrity checked and/or encrypted. The RRC layer indicates to the RANAP layer of the RNC10 if the message was integrity checked and/or ciphered. The fields or other indication indicating if the message is encrypted and/or integrity checked are sent to the RANAP layer of the SGSN 14. in the RANAP header with the message being in the body of the packet. The integrity check itself is, in preferred embodiments of the invention, the indication that an integrity check has been carried out. The MM entity of the SGSN receives the message and indication from the RANAP entity and decides whether or not to accept this message.

In summary, the RNS is not aware of the content of the MM message. Therefore, for downlink packets, an indication is provided to the RNS as to whether or not the message is to be ciphered and/or integrity checked. For uplink packets an indication is provided to the SGSN as to whether or not the message has been ciphered and/or integrity checked.

The integrity check procedure will now be described. Most radio resource control RRC, MM SM information elements are considered sensitive and must be integrity protected. An integrity function is thus applied on these signalling information elements transmitted between the mobile station and the RNS 12. This integrity function uses an integrity algorithm with the integrity key Ik to compute a message authentication code for a given message. This is carried out in the mobile station and the RNS which both have integrity key Ik and the integrity algorithm.

Reference is made to Figure 4 which illustrates the use of the integrity algorithm to authenticate the data integrity of a signalling message.

The input parameters to the algorithm are the integrity key Ik, a time dependent input COUNT-I, a random value generated by the network FRESH, the direction bit DIRECTION and the signalling data MESSAGE. The latter input is the message or packet data. Based on these input parameters, a message authentication code for data integrity (MAC-I) is calculated by the integrity algorithm. This code MAC-I is then appended to the message when sent over the radio access link. either to or from the mobile station The receiver of that code and message also computes a message authentication code for data integrity XMAC-I on the message received using the same algorithm. The algorithm has the same inputs as at the sending end of the message. The code calculated by the algorithm at the sending end and the receiving end should be the same if the data integrity of the message is to be verified.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the hyperframe number (HFN) as the most significant part and a RRC sequence number as the least significant part. The initial value of the hyperframe number is sent by the mobile station to the network during the connection set-up. The mobile station stores the greatest used hyperframe number from the previous connection and increments it by one. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.

The input parameter FRESH protects the network against replay of signalling messages by the mobile station. At connection set-up the network generates a random value FRESH and sends it to the user. The value FRESH is subsequently used by both the network and the mobile station throughout the duration of a

single connection. This mechanism assures the network that the mobile station is not replaying any old message authentication code.

The setting of the integrity key Ik is as described hereinbefore. The key may be changed as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber is known. The key Ik is stored in the visitor location register and transferred to the RNC 10 when it is needed. The key Ik is also stored in the mobile station until it is updated at the next authentication.

A key set identifier KSI is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network. The key set identifier is used to allow key re-use during subsequent connection set-ups. The KSI is used to verify whether the MS and the network are to use the same cipher key and integrity key.

A mechanism is provided to ensure that a particular integrity key is not used for an unlimited period of time, to avoid attacks using compromised keys. Authentication which generates integrity keys is not mandatory at call set-up.

Each time an RRC connection is released the highest value of the hyper-frame number of the bearers that were protected in that RRC connection is stored in the mobile station. When the next RRC connection is established that value is read from the mobile station and incremented by one by a counter.

The mobile station is arranged to trigger the generation of a new cipher key and an integrity key if the counter reaches a maximum value set by the operator and stored in the mobile station at the next RRC connection request message sent out. This mechanism will ensure that an integrity key and cipher key cannot be reused more times than the limit set by the operator.

It should be appreciated that there may be more than one integrity algorithm and information is exchanged between the mobile station and the radio network controllers defining the algorithm. It should be noted the same algorithm should be used by the sender and receiver of messages.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the mobile station which version or versions of the algorithm the MS supports. This message itself must be integrity protected and is transmitted to the RNC after the authentication procedure is complete.

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the mobile station with those indicated by the mobile station and act according to the following rules:

1) If the mobile station and the network have no versions of the algorithm in common, then the connection shall be released.

2) If the mobile station and the network have at least one version of the algorithm in common, then the network shall select one of the mutually acceptable versions of the algorithm for use on that connection.

Integrity protection is performed by appending the message authentication code MAC-I to the message that is to be integrity protected. The mobile station can append the MAC-I to signalling messages as soon as it has received a connection specific FRESH value from the RNC.

If the value of hyper-frame is larger or equal to the maximum value stored in the mobile station, the mobile station indicates to the network in the RRC connection set-up that it is required to initialise a new authentication and key agreement.

RNC may be arranged to detect that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or handover to a new RNC does not support an algorithm selected by the old RNC, etc.

A new cipher key Ck is established each time an authentication protocol is executed between the mobile station and the SGSN.

A plurality of different encryption algorithms may be provided. When an MS wishes to establish a connection with the network, the mobile station shall indicate to the network which version of the encryption algorithm it supports. The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the mobile station, with those indicated by the mobile station and act according to the following rules:

If the mobile station and the network have no versions of the encryption algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

If the mobile station and the network have at least one version of the encryption algorithm in common, then the network shall select one of the mutually acceptable versions of the encryption algorithm for use on that connection.

If the mobile station and the network have no versions of the encryption algorithm in common and the mobile station and the network are willing to use an unciphered connection, then an unciphered connection shall be used.

The integrity key Ik may be changed if there is handoff of the mobile station from one base station to a different base station

The following is a list of L3 messages, which can be sent without any security, if required in embodiments of the invention. For example if key needs to be exchanged during a connection, the new key set up procedure should not be encrypted or integrity checked.

attach request

attach reject – this is when the mobile station is not allowed to attach to the network.

authentication and ciphering request

authentication and ciphering response

authentication and ciphering reject – that is where the mobile station has not been authenticated or there is an ciphering error.

mobile station identity request

mobile station identity response

routing area update request

routing area update reject

service request

service request reject

Without embodiments of the invention, the SGSN MM layer would know if a message is allowed or not to be ciphered or integrity checked but only the RRC knows if the message has been ciphered and/or integrity checked. Embodiments of the invention address this difficulty.

If an integrity check fails, this may be due to reasons other than breach of security such as error in the hyper-frame number. A new authentication procedure may need to be performed and that procedures should not be encrypted or integrity checked.

It should be appreciated that embodiments of the invention, the integrity check may only be commenced at any point after the connection has been set up as well as at attach.

By providing the encryption indication and integrity check fields indication, SGSN can ensure that those MM messages and the like which should not be ciphered and/or integrity checked are not even if they occur after the security mode procedure has been completed. Additionally, the RNS itself does not need to look at the content of the message itself in order to determine if it is the type of message which does or does not require ciphering and/or integrity checking. This is also true for MM messages originating from the mobile station. The SGSN MM entity can check that a message which should have been checked has in fact been checked.

In alternative embodiments of the present invention, any other suitable mechanism may be provided to permit the elements of the network to distinguish between those messages which require ciphering and/or integrity checking and those which do not.

It should be appreciated that with data connections, the connection may be open for relatively long periods of time or may even be permanently open.

The steps of the method described with reference to Figure 3 can be performed in any other suitable order. The order of different functions of the different steps can be altered or form part of different steps.

The embodiments of the present invention have been described in the context of a wireless cellular telecommunications network. However, alternative embodiments of the present invention may be used with any other type of communications network wireless or otherwise. Embodiments of the present

invention may be used any form or communication where encryption and/or integrity checks or the like are provided.

In an alternative embodiment of the invention, the integrity and encryption indication may be replaced by a single security indication.

One embodiment of the invention is applicable only to MM messages in networks where all other L3 messages are always ciphered. However, in embodiments of the invention, the RNS does not distinguish between the different types of L3 messages and treats them the same. Alternative embodiments of the invention may be used in conjunction with any other L3 layer message. Embodiments of the invention may be used with any two or more (even all) L3 messages.

Further embodiments of the invention may be used with other types of messages other than L3 layer messages. Indeed alternative embodiments of the invention may be used with any appropriate nodes of a communication network wireless or otherwise. These nodes in alternative embodiments may include one or more of the nodes described previously or any other type of node. Embodiments of the invention may be used for communications between a first and a third node which are via a second node. Embodiments of the invention may be used where the second node is not able to understand part or all of the messages between the first and third nodes. The second node may be provided with information which it is able to understand. This information may be security information as described hereinbefore or may be any other suitable information. That information may comprise information about the message or information about how the message is to be modified by the second node. The information may be from the first and/or third nodes or from any other source. The information may define the protocol to be used, the type of ciphering to be used or any other indication.

CLAIMS

1. A method of communication between a first node, second node, and a third node comprising the steps of:

providing a message to be transmitted from one of the first and third nodes to the other of said first and third nodes, said message being sent through said second node;

applying any required security procedure;

determining if said message is to have a security procedure applied thereto in the first and/or the third node; and

providing information relating to said security procedure.

2. A method as claimed in claim 1, wherein said information relating to said security procedure comprises information as to the applied security procedure.

3. A method as claimed in claim 1 or 2, wherein said information relating to said security procedure comprises information as to the required security procedure.

4. A method as claimed in any preceding claim, wherein said information is provided between said first and second nodes.

5. A method as claimed in any preceding claim, wherein said security procedure is applied to communications between said second and third nodes.

6. A method as claimed in any preceding claim, wherein said second node is arranged to determine if a security procedure is to be applied based on an indication received from said first node.

7. A method as claimed in any preceding claim, wherein said method is a method of communication in a wireless communications system.

8. A method as claimed in claim 7, wherein at least one of said first and second nodes is a network element.

9. A method as claimed in claim 8, wherein said second node comprises a element for controlling a base station.

10. A method as claimed in claim 8 or 9, wherein said second node comprises a base station.

11. A method as claimed in any of claims 7 to 10 wherein said second node is an RNS.

12. A method as claimed in any preceding claim, wherein said second node is arranged to provide an indication to the first node depending on if a security procedure has been applied to the message received by the second node from the third node.

13. A method as claimed in any preceding claim, wherein said first node provides an indication to the second node as to the security procedure to be used between the second and third nodes.

14. A method as claimed in any of the preceding claims when appended to claim 6, wherein said indication is a RANAP indication.

15. A method as claimed in any preceding claim, wherein said security procedure is an encryption procedure.

16. A method as claimed in any preceding claim, wherein said security procedure is an integrity check.

17. A method as claimed in any preceding claim, wherein said third node is user equipment.

18. A method as claimed in claim 17, wherein the user equipment is a mobile station.

19. A method as claimed in claim 17 or 18, wherein said user equipment, when transmitting to said second node is arranged to provide an indication as to the security procedure applied to said message.

20. A method as claimed in any preceding claim, wherein the first node is a SGSN.

21. A method as claimed in any preceding claim, wherein said second node transmits the message with any required security procedure to said third node with an indication as to if any security procedure has been applied thereto.

22. A method as claimed in any of claims 21, wherein said second node is arranged to read said indication but not said message.

23. A method as claimed in any of claims 21 or 22, wherein said second node is arranged to receive messages from said third node along with the indication as to whether a security procedure was applied thereto and provide the message and said indication to said first node.

24. A method as claimed in claim 23, wherein said indication provided to said first node is a RANAP indication.

25. A method as claimed in claim 23 or 24, wherein said second node is arranged to perform a function with respect to said message in dependence on said indication.

26. A method as claimed in claim 25 when appended to claim 15, wherein said function is to decrypt said message if said message has been encrypted.

27. A method as claimed in claim 26 when appended to claim 16, wherein said function is to perform an integrity check on said message and to compare the result of the check with information received from said first node if the message has been integrity checked.

28. A method as claimed in any preceding claim, wherein said message is a data packet.

29. A communications system comprising a first node and a second node and a third node, at least one of said first and third nodes via said second node, being arranged to transmit a message to be transmitted to the other of said first and third nodes; the transmitting node having means for determining if said message is to have a security procedure applied thereto, means for applying any required security procedure to said message, and means for providing information relating to said security procedure.

30. A node for use in a communications system, said node being arranged to transmit a message from one node to another node, said node having means for receiving information relating to a security procedure to be applied to the message, means for applying said security procedure and means for transmitting the message to the another node.

31. A node for use in a communications system, said node comprising means for transmitting a message from one node to another node, said node receiving information relating to a security procedure applied to said message, and means for advising the another node of said security procedure.

32. A method of communication between a first node, a second node and a third node comprising the steps of:-

providing a message to be transmitted from one of the first and third nodes to the other of the first and third nodes, said message being sent through said second node;

providing said second node with information associated with said message, said second node being arranged to read said information but not said message; and

providing a function associated with said information, if required.

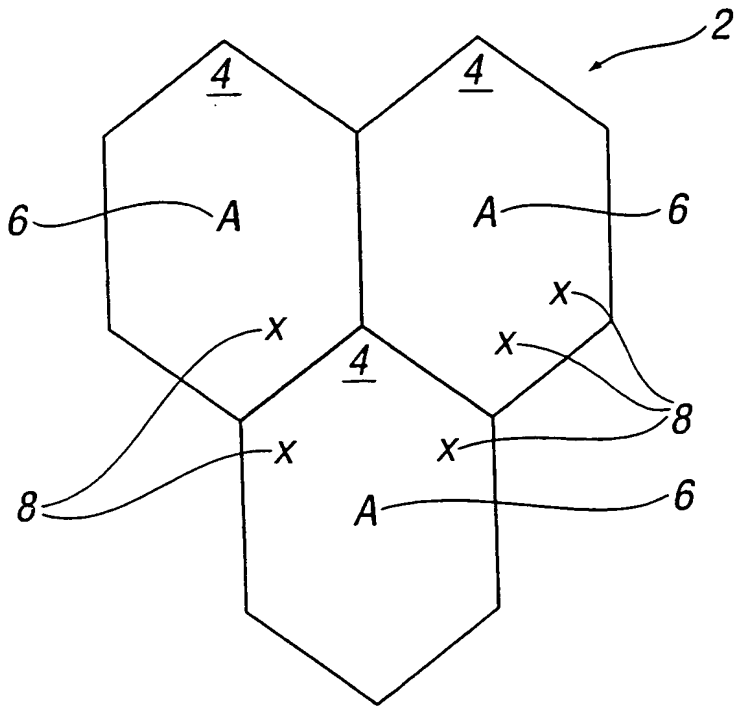


FIG. 1

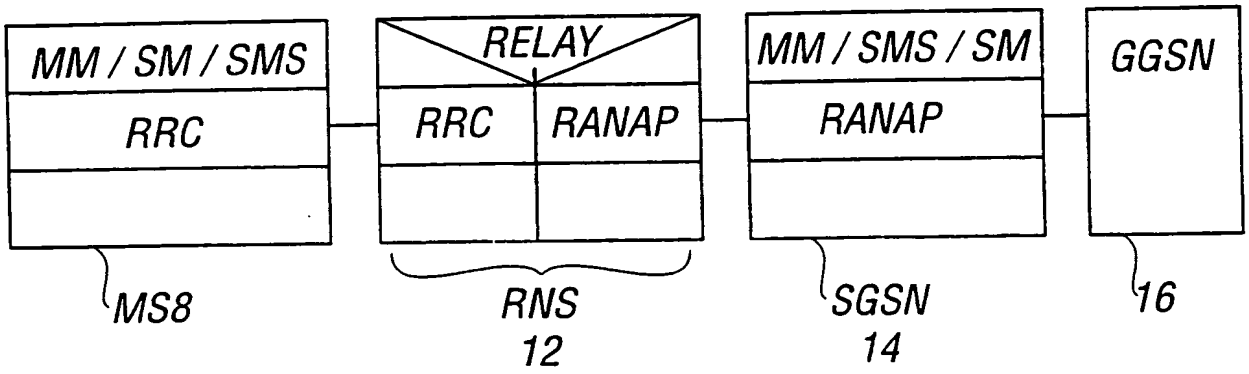


FIG. 2

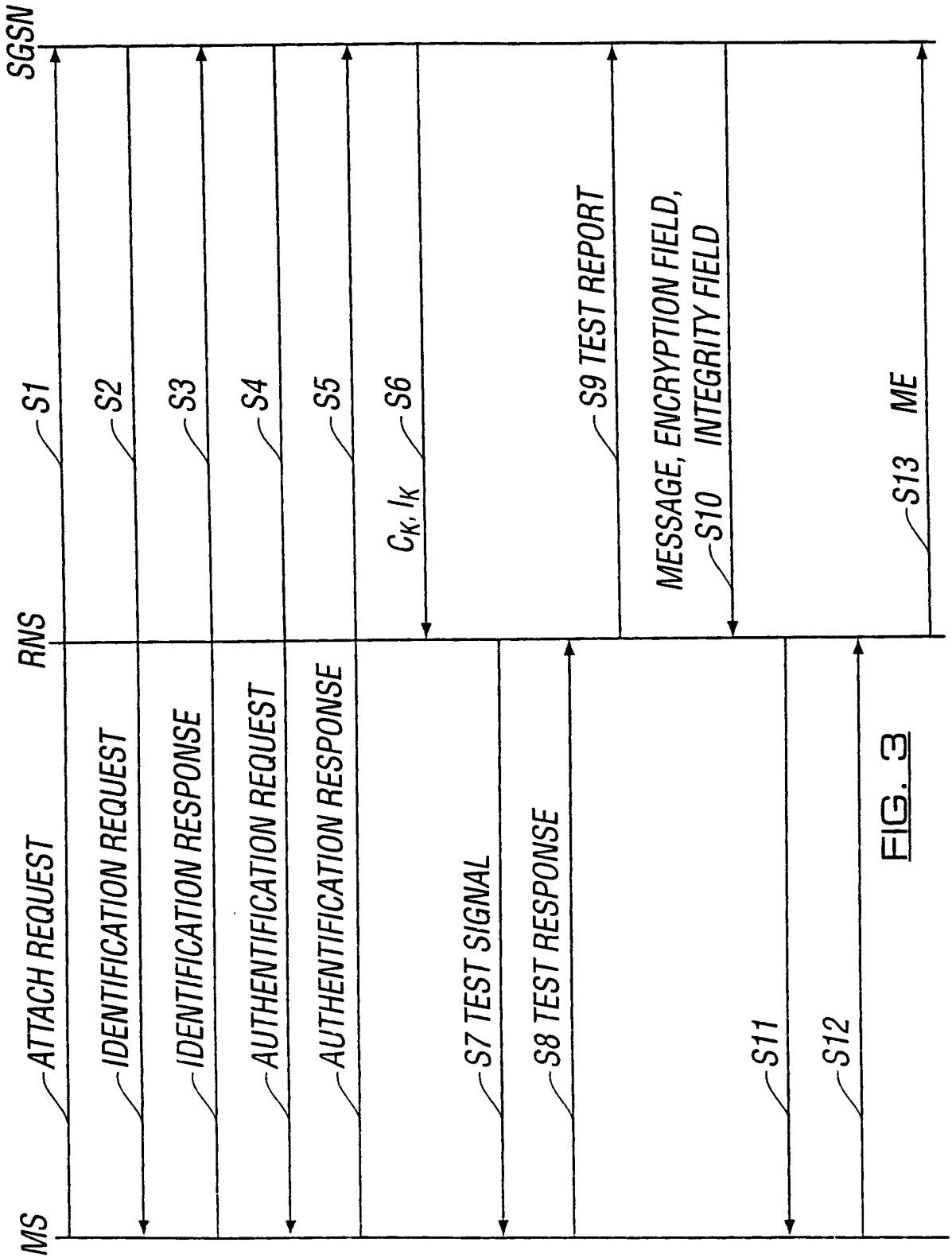


FIG. 3

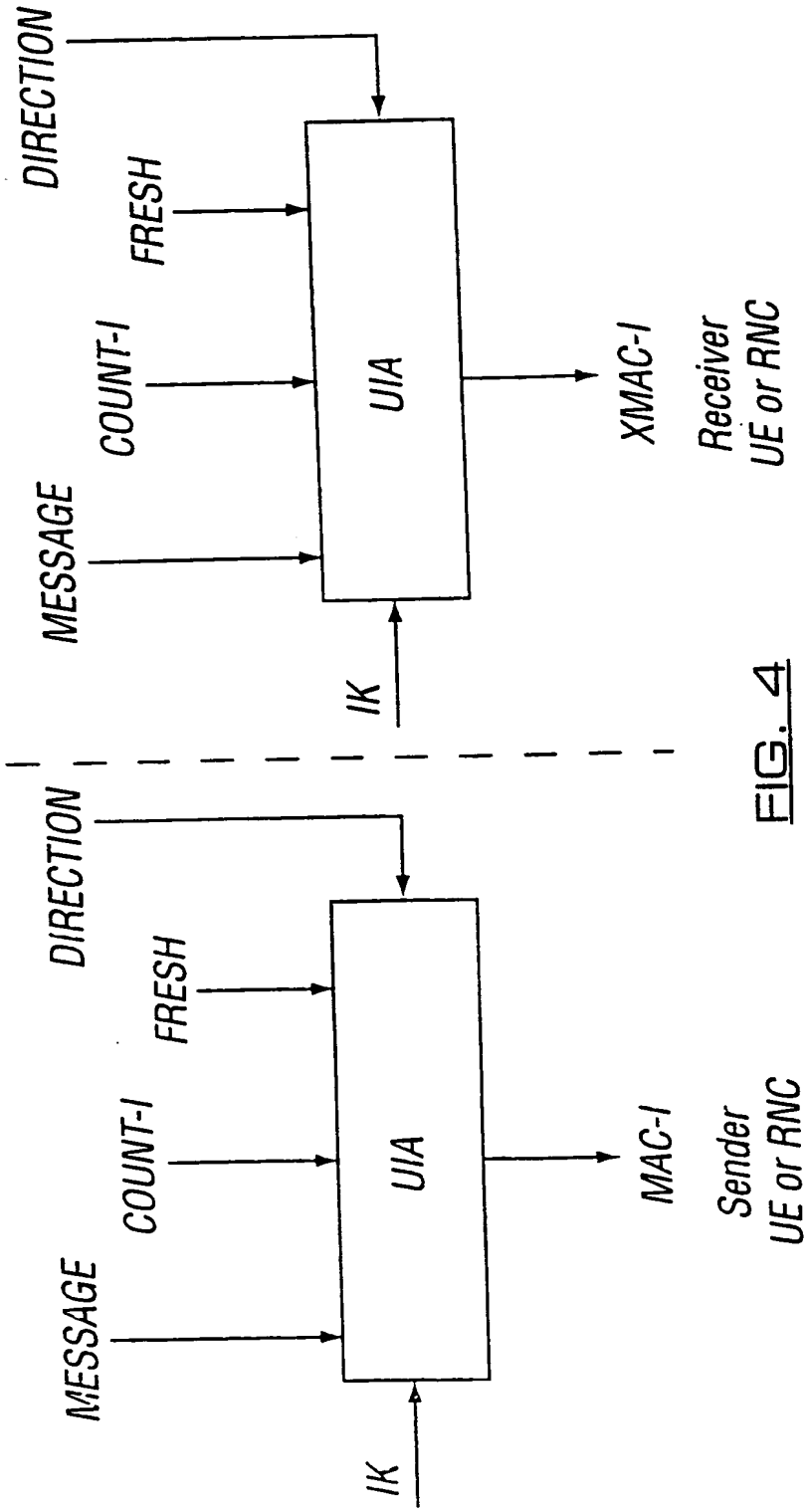


FIG. 4

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 00/11747

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 57465 A (VPNET TECHNOLOGIES INC) 17 December 1998 (1998-12-17)	32
A	page 9, line 1 -page 12; figures 2-4	1,29-31

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February 2001	02/03/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Tsapelis, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/EP 00/11747

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9857465 A	17-12-1998	AU 7837998 A	30-12-1998
		EP 0988735 A	29-03-2000

Form PCT/ISA/210 (patent family annex) (July 1992)